REMARKS

Claims 1-54 remain in this application. Applicants respectfully request reconsideration and review of the application in view of the following remarks.

As an initial matter, Applicants have amended the specification to correct a minor error. Applicants also include an amendment to Fig. 10, in which box 428 is amended to read "Access Allowed." This correction would be consistent with the description at page 18, lines 20-22. A proposed replacement drawing is enclosed. Applicants respectfully submit that these amendments do not add any new matter.

Before addressing the merits of the rejections based on prior art, Applicants provide the following brief description of the invention. The patent application is generally directed to a location-based method of controlling access to digital information. Applicants use the term "location identity" to refer to an attribute of digital information that determines the precise location at which the information can be accessed. The location identity attribute is associated with the digital information in a manner such that a receiving device could only access the digital information when present at the specific geographic location, and would not be able to access the digital information at another location. The terms "associate" or "associating" are generally defined as a combining or joining together, and that is the meaning intended with respect to the associating of the digital information with the location identity attribute. More specifically, the digital information is marked with the location identity attribute in such a matter that the association cannot be lost no matter how the digital information is subsequently transmitted, used or stored. The location identity becomes an inherent attribute of the digital information when this association is made, at which point the digital information is termed to be "geolocked" in the lexicon of the patent application.

A device receiving the geolocked digital information would only be able to access that information at the specific geographic location defined by the location identity attribute. The receiving device would include some means for determining its location,

such as a GPS receiver. If the determined location does not match the location identity associated with the geolocked digital information, the receiving device would be unable to access the digital information. In an embodiment of the invention, the digital information is encrypted using the location identity attribute so that it can only be accessed at the location defined by the location identity. By use of the term "access," Applicants refer to the full range of functions that may be performed with respect to digital information, including saving, storing, copying, deleting, and displaying. As described in the patent application:

> In accordance with the invention, whenever digital information is saved, stored, or copied, a location identity attribute 140 is associated with the digital information so that subsequent access of the digital information is limited to the geographic area specified by the location identity attribute 140.

See page 11, lines 6-9. Thus, the invention permits the interchange of digital information while controlling security and preventing unauthorized access to the information.

The Examiner rejected Claims 1-3, 5-8, 10-12, 15, 16, 24, 25, 27, 28-30, 32-35, 37-39, 42, 43, 51, 52 and 54 under 35 U.S.C. § 102(b) as anticipated by Murphy. The Examiner further rejected Claims 14 and 41 under 35 U.S.C. § 103(a) as unpatentable over Murphy. Applicants respectfully traverse these rejections.

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location stored in the receiver/processor for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is

coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated.

As a fundamental matter, Murphy discloses no association between the digital information and the location identity attribute. Murphy is directed to a one-to-many communication system in which the same encrypted signals are sent to many users. There is nothing distinctive about the encrypted signals that reflects an association with a specific geographic location. In fact, the encrypted signals themselves have no relation to the location information whatsoever. Instead, Murphy uses location information only to determine whether to activate the decryption chip. The SATPS location signal is compared to location information that is previously stored in the receiver, and which has nothing to do with the encrypted signals. Notably, this determination occurs whenever the set-top box (i.e., receiver) is turned on or after the power supply is interrupted (see col. 8, lines 6-24 and 46-62), i.e., without any consideration of the encrypted signals.

Murphy therefore fails to suggest or disclose the step of "associating with said digital information a location identity attribute that defines at least a specific geographic location, wherein said digital information can be accessed only at said specific geographic location," as defined in Claim 1. Likewise, Murphy fails to suggest or disclose "a processor having memory adapted to store software instructions operable to cause said processor to associate with said digital information a location identity attribute that defines at least a specific geographic location, wherein said digital information can be accessed only at said specific geographic location," as defined in Claim 28. The rejection of these claims, and all claims dependent thereon, should therefore be withdrawn.

The Examiner further rejected Claims 4, 9, 31 and 36 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Hastings et al. Applicants respectfully traverse this rejection.

Hastings discloses information files stored in encrypted form on a CD-ROM. The same CD-ROM also contains a list of authorized geographic regions and decryption key files. A table (see, e.g., Table 1) links the encrypted files, the decryption keys necessary to decrypt the encrypted files, and the associated geographic regions in which the keys can be accessed. The computer system includes a GPS receiver, which provides current location information. To operate the system, a user first enters a password. If the password is authentic, the computer compares the location information obtained using the GPS receiver with the list of authorized geographic regions defined in the table. If there is a match, the computer system retrieves the corresponding decryption key from the CD-ROM and uses the key to decrypt the encrypted file authorized for use in that geographic region, thereby enabling the user to access the decrypted file.

As with Murphy described above, Hastings uses location information to determine whether to enable access to stored decryption keys that can decrypt digital information, but there is nothing inherent in the digital information itself that prevents it from being accessed anywhere but the desired location. Hastings uses location information as a form of gate keeper process, in contrast to the present invention in which location identity is an inherent attribute of the stored data.

More particularly, the stored information in Hastings is not "associated" with the location information as that term is used in the present application. The table provides only a cross-reference or arbitrary linkage between the encrypted data files and the authorized geographic regions. The stored information is not marked or altered in any manner to reflect an association with geographic information. In fact, the stored information has no relationship to the location information other than the arbitrary linkage formed by the table and is at all times entirely independent of the location information. Once the stored information is decrypted, the information can be freely disseminated, i.e., copied, stored, displayed, transmitted, etc., because the arbitrary linkage between the encrypted data files and the location information ends. As a result,

Hastings provides no ability to limit access to the stored information at the specific geographic location.

Hastings therefore fails to make up for the significant deficiency of Murphy, and the proposed combination of references thereby fails to suggest or disclose the claims as set forth above. This ground of rejection should also be withdrawn.

The Examiner further rejected Claims 13 and 40 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Emery et al. Applicants respectfully traverse this rejection.

Emery discloses a method for linking telephone numbers and identifiers with geographic location. The reference has no applicability to the present invention and fails to make up for the deficiencies of Murphy discussed above. This ground of rejection should also be withdrawn.

The Examiner further rejected Claims 17-20 and 44-47 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Schipper et al. Applicants respectfully traverse this rejection.

Schipper discloses a method of communicating between mobile stations using present and past location information to vary an encryption key. The mobile stations each have a satellite positioning system (SATPS) receiver and antenna that receive signals from a plurality of navigation satellites. The SATPS receiver generates psuedorange measurements from that station to each navigation satellite in view, and produces location information based on a plurality of pseudorange measurements. Schipper periodically communicates pseudorange correction values (PRC) from a base station to the mobile stations, which in turn use these pseudorange correction values to correct their own location determinations. By design, Schipper purposefully eliminates location from the correction values by calculating them as the differential between the known base station location and the SATPS pseudorange measurements. The mobile states also use the pseudorange correction values as a parameter to determine the encryption key for messages transmitted to other mobile stations. The pseudorange

correction values can be used as an encryption key because they represent a convenient mathematical value known to each of the mobile stations that changes over time to provide added security.

According to the Examiner, "Schipper discloses an apparatus for location specific encryption/decryption of a signal wherein communications are encrypted/decrypted by a key based on one or more location identity attributes." This conclusion is not correct. The pseudorange correction values do not uniquely identify a geographic location, but instead represent the difference between the known location of the fixed station and the calculated location. In other words, Schipper starts with an accurate determination of location, and then subtracts out the location calculation to get the pseudorange correction values, which are essentially "noise." Schipper then uses the "noise" as the common encryption key. Moreover, the pseudorange correction values are common to all mobile stations that communicate with the fixed station (see col. 8, lines 23-28), and do not constitute the "location of the mobile station at a given time" as stated by the Examiner. It is therefore erroneous for the Examiner to consider the pseudorange correction values as analogous to a location identity attribute.

More particularly, the pseudorange correction values do not define "at least a specific geographic location" as defined in Claims 1 and 28, because they constitute information common to a broad geographic region. Schipper thus fails to make up for deficiency of Murphy described above insofar as the reference fails to suggest or disclose the step of "associating with said digital information a location identity attribute that defines at least a specific geographic location," as defined in Claim 1, or "software instructions operable to cause said processor to associate with said digital information a location identity attribute that defines at least a specific geographic location," as defined in Claim 28. In addition, the proposed combination of references fails to suggest or disclose "encrypting said digital information using an encryption key based at least in part on said location identity attribute," as defined in Claim 17, or "software instructions operable to cause said processor to encrypt said digital information using an encryption

key based at least in part on said location identity attribute," as defined in Claim 44. The rejection of these claims, and all claims dependent thereon, should therefore be withdrawn.

The Examiner further rejected Claims 21-23, 26, 48-50 and 53 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Shimada. Applicants respectfully traverse this rejection.

Shimada discloses a data processing method in which access to information is controlled using a password and location attribute data. A data file includes fields for the attachment of attributes defining a password and location. When it is desired to access the data file, a data processing system compares the attached password to one inputted by a user, and also compares the attached location data to a current location determined by a location determining system (e.g., GPS). If the password is correct and the location matches, then access to the data file is permitted.

As with Hastings discussed above, Shimada provides a mere gatekeeper function in allowing/disallowing access to information, but does not "associate" the information with location as that term is used in the present application. The attached attribute data provides only an arbitrary linkage with the data files. Once the data files are accessed, the information can be freely disseminated, i.e., copied, stored, displayed, transmitted, etc., because the arbitrary linkage between the data files and the location information ends. As a result, Shimada provides no ability to limit access to the stored information at the specific geographic location. Shimada therefore fails to make up for the deficiencies of Murphy described above, and this ground of rejection should also be withdrawn.

In view of the foregoing, Applicants respectfully submit that Claims 1-54 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

Applicants petition the Commissioner for a one-month extension of time, extending to November 23, 2004, the period for response to the Office Action dated July 23, 2004. A check in the amount of $55.00 is enclosed for the one-month extension of time pursuant to 37 CFR §1.17(a)(1). The Commissioner is authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,

Date: November 17, 2004

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000

Enclosure: Replacement Drawing (Fig. 10)